

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

EDMUND METZGER, individually and on behalf of others Civil Action No.:
similarly situated,

Plaintiff,

**CLASS ACTION
COMPLAINT**

-against-

T-MOBILE USA, INC,

Defendant.

-----X

Plaintiff Edmund Metzger (“Plaintiff”), individually and on behalf of all others similarly situated (the “Class” or “Class members”), brings this Class Action Complaint against Defendant T-Mobile USA, Inc., based upon his individual experiences and personal information, and investigation by his counsel.

INTRODUCTION

1. Plaintiff, individually and on behalf of all others similarly situated, brings this class action suit against Defendant because of Defendant’s failure to safeguard the confidential information of millions of current and former T-Mobile USA, Inc. customers. The confidential information stolen appears to be encompass names, birthdays, Social Security numbers, driver’s license numbers, phone numbers, and account PIN’s, among other Personal Identifying Information (PII).

2. T-Mobile USA, Inc. (hereinafter T-Mobile) is a nationwide telecommunications company headquartered in Bellevue, Washington and is a wholly owned subsidiary of Deutsche Telekom AG, headquartered in Bonn, Germany With over ninety-five million customers in the United States, T-Mobile collects a significant amount of data from its current and former customers, often including sensitive personal information such as Social Security numbers, addresses,

telephone numbers, dates of birth, bank account numbers, credit card numbers, financial transaction records, credit ratings and driver's license numbers.

3. On or about August 19, 2021, T-Mobile announced by a "Notice of Data Breach" on its website that it had learned on August 17, 2021 that "a bad actor illegally accessed personal data." It was not stated when the breach itself occurred.

4. The confidential information that was compromised in the Data Breach can be used to gain unlawful access to the users' other online accounts, carry out identity theft, or commit other fraud and can be disseminated on the internet, available to those who broker and traffic in stolen PII.

5. While the sophistication of the methods employed in effectuating the Data Breach is not publicly known, it is certain that the Data Breach could have been avoided through basic security measures, authentications, and training.

6. At all relevant times, Defendants promised and agreed in various documents to safeguard and protect Personal Identifiable Information (PII) in accordance with federal, state, and local laws, and industry standards, including the New York SHIELD Act. Defendants made these promises and agreements on their websites and other written notices and also extended this commitment to situations in which third parties handled PII on their behalf.

7. Contrary to these promises, and despite the fact that the threat of a data breach has been a well-known risk to Defendant, which has experienced data breaches in the past, especially due to the valuable and sensitive nature of the data Defendant collects, stores and maintains, Defendant failed to take reasonable steps to adequately protect the PII of its current and former customers. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect PII.

8. As a result of Defendant's failure to take reasonable steps to adequately protect the PII of current and former T-Mobile customers, Plaintiff's and Class members' PII is now on the internet for anyone and everyone to acquire, access, and use for unauthorized purposes for the foreseeable future.

9. Defendant's failure to implement and follow basic security procedures has resulted in ongoing harm to Plaintiff and Class members who will continue to experience a lack of data security for the indefinite future and remain at serious risk of identity theft and fraud that would result in significant monetary loss and loss of privacy.

10. Accordingly, Plaintiff seeks to recover damages and other relief resulting from the Data Breach, including but not limited to, compensatory damages, reimbursement of costs that Plaintiff and others similarly situated will be forced to bear, and declaratory judgment and injunctive relief to mitigate future harms that are certain to occur in light of the scope of this breach.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds \$5 million, exclusive of interest and costs; the number of members of the proposed Class exceeds 100; and diversity exists because Plaintiff and Defendants are citizens of different states. Subject matter jurisdiction is also based upon the Federal Trade Commission Act (FTCA). This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

12. This Court has personal jurisdiction over Defendant as it conducts substantial business in this State and in this District and/or the conduct complained of occurred in and/or emanated from this State and District because the confidential information compromised in the Data Breach was likely stored and/or maintained in accordance with practices emanating from this

District.

13. Venue is proper pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the conduct alleged in this Complaint occurred in, were directed to, and/or emanated from this District, and because Plaintiff resides within this District.

THE PARTIES

14. Plaintiff Edmund Metzger is an individual T-Mobile customer residing in the County of Kings, State of New York.

15. Defendant T-Mobile is a telecommunications company, a wholly owned subsidiary of Deutsche Telekom AG, authorized to conduct business in the State of New York, which conducts business within the State of New York and within this District, with its headquarters located in Bellevue, Washington.

FACTUAL ALLEGATIONS

16. At all pertinent times, Plaintiff was a customer of T-Mobile, having purchased telecommunications services and devices. In the course of said purchases, Plaintiff was required to provide certain personal and financial information to T-Mobile, including name, address, Social Security number, vehicle information, credit card numbers and driver's license number.

17. On or about August 19, 2021, Defendant T-Mobile advised Plaintiff via its website that a data breach had occurred, resulting in unknown actors gaining access to and stealing PII.

18. Plaintiff and Class members were required to agree to T-Mobile's Privacy Policy, Terms of Use, Payment Authorization, and Consent to Electronic Transactions and Disclosures.

19. T-Mobile promised to protect the PII of its policyholders and emphasizes its purported commitment to protection of PII. T-Mobile's website claims:

We use administrative, technical, contractual, and physical safeguards designed to protect your data while it is under our control. For example, when you contact us by phone or visit us in our stores, we have procedures in place to make sure that only the primary account holder or authorized users have access.

20. T-Mobile has failed to maintain the confidentiality of PII, failed to prevent cybercriminals from access and use of PII, failed to avoid accidental loss, disclosure, or unauthorized access to PII, failed to prevent the unauthorized disclosure of PII, and failed to provide security measures consistent with industry standards for the protection of PII, of its current and former customers.

21. The “Notice of Data Breach” dated August 19, 2021 stated the breach was discovered on August 17, 2021, but did not state when the breach was believed to have occurred.

22. This data breach was foreseeable, in light of the much-publicized wave of data breaches in recent years. Since at least 2015, the Federal Bureau of Investigation (“FBI”) has specifically advised private industry about the threat of “Business E-Mail Compromise” (“BEC”). The FBI calls BEC “a growing financial fraud that is more sophisticated than any similar scam the FBI has seen before and one—in its various forms—that has resulted in actual and attempted losses of more than a billion dollars to businesses worldwide.” The FBI notes that “scammers’ methods are extremely sophisticated,” and warns companies that “the criminals often employ malware to infiltrate company networks.”¹ T-Mobile has also experienced data breaches in the past.

23. Accordingly, T-Mobile knew, given the vast amount of PII it collects, manages, and maintains, that they were targets of security threats, and therefore understood the risks posed by unsecure data security practices and systems. Defendant’s failure to heed warnings and to otherwise

¹ BUSINESS E-MAIL COMPROMISE: AN EMERGING GLOBAL THREAT, <https://www.fbi.gov/news/stories/business-e-mail-compromise> (last visited Apr. 20, 2020).

maintain adequate security practices resulted in this Data Breach.

24. Defendant, at all relevant times, had a duty to Plaintiff and Class members to properly secure their PII, encrypt and maintain such information using industry standard methods, train their employees, utilize available technology to defend their systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff and Class members, and promptly notify Plaintiff and Class members when Defendant became aware of the potential that its current and former customers' PII may have been compromised.

25. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant, on the one hand, and Plaintiff and the Class members, on the other hand. The special relationship arose because Plaintiff and the members of the Class entrusted Defendant with their PII as part of receiving telecommunications services and devices from T-Mobile. Defendant had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite their obligation to protect such information. Accordingly, Defendant breached their common law, statutory, and other duties owed to Plaintiff and Class members.

26. Defendant's duty to use reasonable security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data by entities such as Defendant.

27. Defendant's duty to use reasonable security measures also arose under New York's SHIELD Act (General Business Law § 899-bb), requiring businesses that collect private information on New York residents to implement reasonable cybersecurity safeguards to protect that information. It mandates the implementation of a data security program, including measures

such as risk assessments, workforce training and incident response planning and testing, and became effective on or about March 21, 2020. It covers all employers, individuals or organizations, regardless of location, that collect private information on New York residents.

28. The Federal Trade Commission has established data security principles and practices for businesses as set forth in its publication, *Protecting Personal Information: A Guide for Business*.² Among other things, the FTC states that companies should encrypt information stored on computer networks and dispose of consumer information that is no longer needed. The FTC also says to implement policies for installing vendor-approved patches to correct problems, and to identify operating systems. The FTC also recommends that companies understand their network's vulnerabilities and develop and implement policies to rectify security deficiencies. Further, the FTC recommends that companies utilize an intrusion detection system to expose a data breach as soon as it occurs; monitor all incoming traffic for activity that might indicate unauthorized access into the system; monitor large amounts of data transmitted from the system, and have a response plan ready in the event of a data breach. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." (17 C.F.R. § 248.201 (2013)).

29. The FTC has prosecuted a number of enforcement actions against companies for failing to take measures to adequately and reasonably protect consumer data. The FTC has viewed

² https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_protecting-personal-information.pdf (last visited Apr. 18, 2020).

and treated such security lapses as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45.

30. Defendant failed to maintain reasonable data security procedures and practices.

31. Accordingly, Defendant did not comply with state and federal law requirements and industry standards, as discussed above.

32. Defendant was at all times fully aware of its obligations to protect the PII of current and former customers. Defendant was also aware of the significant consequences that would result from its failure to do so.

33. To date, Defendant has merely advised customers of identity theft and credit monitoring services to which they may subscribe, with no charge to T-Mobile customers. The offer, however, is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and it entirely fails to provide any compensation for the unauthorized release and disclosure of Plaintiff’s and Class Members’ PII.

34. Furthermore, Defendant’s monitoring offer to Plaintiff and Class Members squarely places the burden on Plaintiff and Class Members, rather than upon the Defendant, to investigate and protect themselves from Defendant’s tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiff and Class members in monitoring services upon discovery of the breach, Defendant merely sent instructions offering the services to potentially affected customers with the recommendation that they sign up for the services.

35. As a result of the data breach and Defendant’s failure to provide timely notice to Plaintiff and Class members, Plaintiff’s and Class members’ PII are now in the hands of unknown hackers, and Plaintiff and Class members now face an imminent, heightened, and substantial risk

of identity theft and other fraud, which is a concrete and particularized injury traceable to Defendants' conduct. Accordingly, Plaintiffs and the Class members have suffered "injury-in-fact." See *Attias v. CareFirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017).

36. As a direct and proximate result of Defendant's wrongful actions and inaction, Plaintiff and Class members have suffered injury and damages, including the increased risk of identity theft and identity fraud, improper disclosure of PII, the time and expense necessary to mitigate, remediate, and sort out the increased risk of identity theft and to deal with governmental agencies.

CLASS ACTION ALLEGATIONS

37. Plaintiff brings this action and seeks to certify and maintain it as a class action under Federal Rules of Civil Procedure 23(a), (b)(2), (b)(3), and/or (c)(4), on behalf of himself, and the following proposed Classes (collectively, the "Class").

38. The Nationwide Class is defined as follows: All individuals residing in the United States whose PII was compromised in the data breach initially disclosed by T-Mobile on or about August 19, 2021.

39. The New York Class is defined as follows: All individuals residing in New York whose PII was compromised in the data breach initially disclosed by T-Mobile on or about August 19, 2021.

40. Excluded from each of the above proposed Classes are: Defendant, any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendant; and judicial officers to whom this case is assigned and their immediate family members.

41. Plaintiff reserves the right to re-define the Class definitions after conducting discovery.

42. Each of the proposed Classes meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and/or (c)(4).

43. Numerosity. Fed. R. Civ. P. 23(a)(1). Pursuant to Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiff at this time, the proposed Class includes potentially over fifty millions of individuals whose PII was compromised in the Data Breach. Class members may be identified through objective means, including by and through Defendant's business records. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

44. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). Pursuant to Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include:

- (a) Whether Defendant had a legal duty to implement and maintain reasonable security procedures and practices for the protection of Class members' personal and financial information, including by vendors;
- (b) Whether Defendant breached its legal duty to implement and maintain reasonable security procedures and practices for the protection of Plaintiff and Class members' PII;
- (c) Whether Defendant's conduct, practices, actions, and omissions, resulted in or were the proximate cause of the data breach, resulting in the loss of PII of Plaintiff and Class members;

- (d) Whether Defendant had a legal duty to provide timely and accurate notice of the data breach to Plaintiff and Class members;
- (e) Whether Defendant breached its duty to provide timely and accurate notice of the data breach to Plaintiff and Class members;
- (f) Whether and when Defendant knew or should have known that its computer systems were vulnerable to attack;
- (g) Whether Defendant failed to implement and maintain reasonable and adequate security measures, procedures, and practices to safeguard Plaintiff's and Class members' PII, including by vendors;
- (h) Whether Defendant breached express or implied contracts with Plaintiff and the Class in failing to have adequate data security measures despite promising to do so;
- (i) Whether Defendant's conduct was negligent;
- (j) Whether Defendant's conduct was *per se* negligent;
- (k) Whether Defendant's practices, actions, and omissions constitute unfair or deceptive business practices;
- (l) Whether Plaintiff and Class members suffered legally cognizable damages as a result of Defendant's conduct, including increased risk of identity theft and loss of value of their personal and financial information; and
- (m) Whether Plaintiff and Class members are entitled to relief, including damages and equitable relief.

45. Typicality. Fed. R. Civ. P. 23(a)(3). Pursuant to Rule 23(a)(3), Plaintiff's claims are typical of the claims of the members of the Class. Plaintiff, like all members of the Class, were injured through Defendant's uniform misconduct described above and asserts similar claims for

relief. The same events and conduct that give rise to Plaintiff's claims also give rise to the claims of every other Class member because Plaintiff and each Class member are persons that have suffered harm as a direct result of the same conduct engaged in by Defendant and resulting in the data breach.

46. Adequacy of Representation (Fed. R. Civ. P. 23(a)(4)). Pursuant to Rule 23(a)(4), Plaintiff and his counsel will fairly and adequately represent the interests of the Class members. Plaintiff has no interest antagonistic to, or in conflict with, the interests of the Class members. Plaintiff's attorneys are highly experienced in the prosecution of consumer class actions and data breach cases.

47. Superiority (Fed. R. Civ. P. 23(b)(3)). Pursuant to Rule 23(b)(3), a class action is superior to individual adjudications of this controversy. Litigation is not economically feasible for individual members of the Class because the amount of monetary relief available to individual Plaintiffs is insufficient in the absence of the class action procedure. Separate litigation could yield inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. A class action presents fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

48. Risk of Inconsistent or Dispositive Adjudications and the Appropriateness of Final Injunctive or Declaratory Relief (Fed. R. Civ. P. 23(b)(1) and (2)). In the alternative, this action may properly be maintained as a class action, because:

(a) The prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudication with respect to individual members of the Class, which would establish incompatible standards of conduct for Defendants; or

(b) The prosecution of separate actions by individual members of the Class would create a risk of adjudications with respect to individual members of the Class which would, as a practical matter,

be dispositive of the interests of other members of the Class not parties to the adjudications, or substantially impair or impede their ability to protect their interests; or

(c) Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive or corresponding declaratory relief with respect to the Class as a whole.

49. Issue Certification (Fed. R. Civ. P. 23(c)(4)). In the alternative, the common questions of fact and law, set forth above, are appropriate for issue certification on behalf of the proposed Class.

FIRST CAUSE OF ACTION FOR NEGLIGENCE

(on behalf of Plaintiff, the Nationwide Class and the New York Class)

50. The Plaintiff repeats, reiterates and realleges each and every allegation set forth in paragraphs “1” to “49” above as if set forth in full herein.

51. Defendant required Plaintiff and Class members to submit non-public, sensitive PII for purposes of obtaining telecommunications services and devices.

52. Defendant had, and continues to have, a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting their PII. Defendant also had, and continues to have, a duty to use ordinary care in activities from which harm might be reasonably anticipated, such as in the storage and protection of PII within their possession, custody and control and that of its vendors.

53. Defendant’s duty to use reasonable security measures arose as a result of the special relationship that existed between T-Mobile and its customers. Only Defendant was in a position to ensure that its systems were sufficient to protect against the harm to Plaintiff and the Class members from a data breach.

54. Defendant violated these standards and duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect the PII entrusted to it, including Plaintiff's and Class members' PII. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII.

55. Defendant, by and through its negligent actions, inaction, omissions, and want of ordinary care, unlawfully breached its duties to Plaintiff and Class members by, among other things, failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII within their possession, custody and control.

56. Defendant, by and through its negligent actions, inactions, omissions, and want of ordinary care, further breached its duties to Plaintiff and Class members by failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit their processes, controls, policies, procedures, protocols, and software and hardware systems for complying with the applicable laws and safeguarding and protecting their PII.

57. But for Defendant's negligent breach of the above-described duties owed to Plaintiff and Class members, its PII would not have been released, disclosed, and disseminated without its authorization.

58. Plaintiff's and Class members' PII was transferred, sold, opened, viewed, mined and

otherwise released, disclosed, and disseminated to unauthorized persons without their authorization as the direct and proximate result of Defendant's failure to design, adopt, implement, control, direct, oversee, manage, monitor and audit its processes, controls, policies, procedures and protocols for complying with the applicable laws and safeguarding and protecting Plaintiff's and Class members' PII.

59. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the data breach, Plaintiff and Class members have suffered, and will continue to suffer, ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

60. Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused this data breach constitute negligence.

SECOND CAUSE OF ACTION FOR NEGLIGENCE *PER SE*

(on behalf of Plaintiff, the Nationwide Class and the New York Class)

61. The Plaintiff repeats, reiterates and realleges each and every allegation set forth in paragraphs "1" to "60" above as if set forth in full herein.

62. Pursuant to the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security to safeguard

the personal and financial information of Plaintiff and Class members.

63. The FTCA prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the PII of Plaintiff and Class members. The pertinent FTC publications and orders form part of the basis of Defendant’s duty in this regard.

64. Defendant required, gathered, and stored personal and financial information of Plaintiff and Class members for sales and service purposes.

65. Defendant violated the FTCA by failing to use reasonable measures to protect the PII of Plaintiff and Class members and not complying with applicable industry standards, as described herein.

66. Plaintiff and Class members are within the class of persons that the FTC Act was intended to protect.

67. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class members.

68. As a direct and proximate result of Defendant’s negligence *per se*, Plaintiff and Class members have suffered, and continue to suffer, injuries, damages arising from identity theft; from their needing to contact agencies administering unemployment benefits; potentially defending themselves from legal action based upon fraudulent applications for unemployment benefits made in their name; contacting their financial institutions; loss of use of funds; closing or modifying financial accounts; damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives; closely reviewing and monitoring their accounts for unauthorized

activity which is certainly impending; placing credit freezes and credit alerts with credit reporting agencies; and damages from identity theft, which may take months or years to discover and detect.

69. Defendant's violation of the FTCA constitutes negligence *per se*.

70. For the same reasons and upon the same bases, Defendant's violation of the New York SHIELD Act and New York GBL §349 constitutes negligence *per se*.

THIRD CAUSE OF ACTION FOR BREACH OF CONTRACT

(on behalf of Plaintiff, the Nationwide Class and the New York Class)

71. The Plaintiff repeats, reiterates and realleges each and every allegation set forth in paragraphs "1" to "70" above as if set forth in full herein.

72. Plaintiff and Class members, upon information and belief, entered into express contracts with T-Mobile that included T-Mobile's promise to protect nonpublic PII provided to T-Mobile from disclosure.

73. There was offer, acceptance and consideration, the consideration being the payments paid by Plaintiff and Class members in exchange for telecommunication services and devices, including the provisions of those agreements pertaining to the protection of PII.

74. Plaintiff and Class members have performed and satisfied all of their obligations to T-Mobile, pursuant to their customer agreements, except for those obligations they were prevented or excused from performing or satisfying.

75. Defendant breached their contractual obligations to protect the nonpublic PII they possessed and with which they were entrusted with when the information was accessed by unauthorized persons as part of the data breach.

76. As a direct and proximate result of Defendant's breach of contract, Plaintiff and Class members have suffered, and continue to suffer, injuries, damages arising from identity theft;

from their needing to contact agencies administering unemployment benefits; potentially defending themselves from legal action base upon fraudulent applications for unemployment benefits made in their name; contacting their financial institutions; loss of use of funds; closing or modifying financial accounts; damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives; closely reviewing and monitoring their accounts for unauthorized activity which is certainly impending; placing credit freezes and credit alerts with credit reporting agencies; and damages from identity theft, which may take months or years to discover and detect.

77. The above constitutes breach of contract by Defendant.

FOURTH CAUSE OF ACTION FOR BREACH OF IMPLIED CONTRACT

(on behalf of Plaintiff, the Nationwide Class and the New York Class)

78. The Plaintiff repeats, reiterates and realleges each and every allegation set forth in paragraphs “1” to “77” above as if set forth in full herein.

79. Defendant required Plaintiff and Class members to provide PII as a condition of obtaining telecommunication services and devices. In so doing, Plaintiff and Class members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class members if their data had been breached and compromised, or stolen.

80. Plaintiff and Class members fully performed their obligations under the implied contracts with Defendant.

81. Defendant breached the implied contracts it made with Plaintiff and Class members by failing to safeguard and protect their PII, and by failing to provide timely and accurate notice to them that PII was compromised as a result of the data breach.

82. As a direct and proximate result of Defendant’s breach of implied contract, Plaintiff

and Class members have suffered, and continue to suffer, injuries, damages arising from identity theft; from their needing to contact agencies administering unemployment benefits; potentially defending themselves from legal action based upon fraudulent use of their PII; contacting their financial institutions; loss of use of funds; closing or modifying financial accounts; damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives; closely reviewing and monitoring their accounts for unauthorized activity which is certainly impending; placing credit freezes and credit alerts with credit reporting agencies; and damages from identity theft, which may take months or years to discover and detect.

83. The above constitutes breach of implied contract by Defendant.

FIFTH CAUSE OF ACTION FOR MISREPRESENTATION

(on behalf of Plaintiff, the Nationwide Class and the New York Class)

84. The Plaintiff repeats, reiterates and realleges each and every allegation set forth in paragraphs “1” to “83” above as if set forth in full herein.

85. A special, privity-like relationship existed between Defendant and Plaintiff and Class members herein by virtue of their relationship as recipient of PII and provider of PII, imposing a duty upon Defendant to impart correct information to Plaintiff and Class members.

86. The Defendant incorrectly represented to Plaintiff and Class members that they would take appropriate measures to safeguard their PII and promptly notify them of a data breach.

87. Plaintiff and Class members reasonably relied upon said representations in that they held Defendant in a position of trust as recipient of their PII.

88. As a direct and proximate result of Defendant’s misrepresentation, Plaintiff and Class members have suffered, and continue to suffer, injuries, damages arising from identity theft; from their needing to contact agencies administering unemployment benefits; potentially defending

themselves from legal action base upon fraudulent use of their PII; contacting their financial institutions; loss of use of funds; closing or modifying financial accounts; damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives; closely reviewing and monitoring their accounts for unauthorized activity which is certainly impending; placing credit freezes and credit alerts with credit reporting agencies; and damages from identity theft, which may take months or years to discover and detect.

89. The above constitutes misrepresentation on the part of Defendants.

SIXTH CAUSE OF ACTION FOR BREACH OF FIDUCIARY DUTY

(on behalf of Plaintiff, the Nationwide Class and the New York Class)

90. The Plaintiff repeats, reiterates and realleges each and every allegation set forth in paragraphs “1” to “89” above as if set forth in full herein.

91. A fiduciary relationship existed between Plaintiff and Class members and Defendant, in that Defendants were in a position of trust with respect to Plaintiffs and Class members as recipients of Plaintiff’s and Class members’ PII, and owed a duty to insure that the PII entrusted to them was safeguarded pursuant to common law and statute.

92. The Defendant engaged in misconduct, consisting of the failure to safeguard the PII of Plaintiff and Class members that had been entrusted to them, in violation of the duty to exercise due care, its contractual obligations and its statutory obligations pursuant to the Federal Trade Commission Act (“FTCA”), the New York SHIELD Act, New York GBL §349(a) and other statutes.

93. As a direct and proximate result of Defendant’s breach of fiduciary duty, Plaintiff and Class members have suffered, and continue to suffer, injuries, damages arising from identity theft; from their needing to contact governmental agencies; potentially defending themselves from legal action base upon fraudulent use of their PII; contacting their financial institutions; loss of use of funds; closing or modifying financial accounts; damages from lost time and effort to mitigate the

actual and potential impact of the data breach on their lives; closely reviewing and monitoring their accounts for unauthorized activity which is certainly impending; placing credit freezes and credit alerts with credit reporting agencies; and damages from identity theft, which may take months or years to discover and detect.

94. The above constitutes breach of fiduciary duty on the part of Defendant.

SEVENTH CAUSE OF ACTION FOR VIOLATION OF NEW YORK GENERAL

BUSINESS LAW §349

(on behalf of Plaintiff, the Nationwide Class and the New York Class)

95. The Plaintiff repeats, reiterates and realleges each and every allegation set forth in paragraphs “1” to “94” above as if set forth in full herein.

96. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

- (a) Defendant misrepresented material facts to Plaintiff and Class members by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff’s and Class members’ PII from unauthorized disclosure, release, data breaches, and theft;
- (b) Defendant misrepresented material facts to Plaintiff and Class members by representing that it did and would comply with the requirements of federal and state laws pertaining to the privacy and security of Plaintiff’s and Class members’ PII;
- (c) Defendant omitted, suppressed, and concealed material facts of the inadequacy of its privacy and security protections for Plaintiff’s and Class members’ PII;
- (d) Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Plaintiff’s and Class members’ PII, in violation of duties

imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45);

(e) Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to the Plaintiff and the Class in a timely and accurate manner, contrary to the duties imposed by N.Y. Gen. Bus. Law §§ 899-aa(2) and 899-bb (SHIELD Act).

97. Defendant's failure constitutes false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiff and Class members) regarding the security of its network and aggregation of PII.

98. The misrepresentations upon which consumers (including Plaintiff and Class members) relied were material misrepresentations (*e.g.*, as to Defendant's adequate protection of PII), and consumers (including Plaintiff and Class members) relied upon those representations to their detriment.

99. Defendant's conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances. As a direct and proximate result of Defendant's conduct, Plaintiff and other Class members have been harmed, in that they were not timely notified of the data breach, which resulted in profound vulnerability to their personal information and other financial accounts.

100. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and omissions, Plaintiff's and Class members' PII was disclosed to third parties without authorization, causing and will continue to cause Plaintiff and Class members damages.

101. As a direct and proximate result of Defendant's violation of NY GBL §349, Plaintiff and Class members have suffered, and continue to suffer, injuries, damages arising from identity theft; from their needing to contact governmental agencies; potentially defending themselves from legal action based upon fraudulent use of their PII; contacting their financial institutions; loss of use of funds; closing or modifying financial accounts; damages from lost time and effort to mitigate the

actual and potential impact of the data breach on their lives; closely reviewing and monitoring their accounts for unauthorized activity which is certainly impending; placing credit freezes and credit alerts with credit reporting agencies; and damages from identity theft, which may take months or years to discover and detect.

102. The above constitutes violation of NY GBL §349.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the members of the Classes defined above, respectfully request that this Court:

- A. Certify this case as a class action under Federal Rule of Civil Procedure 23, appoint Plaintiff as the Class representative, and appoint the undersigned as Class counsel;
- B. Order appropriate relief to Plaintiff and the Classes;
- C. Enter injunctive and declaratory relief as appropriate under the applicable law;
- D. Award Plaintiff and the Classes compensatory and punitive damages
- E. Award Plaintiff and the Classes pre-judgment and/or post-judgment interest as prescribed by law;
- F. Award reasonable attorneys' fees and costs as permitted by law; and
- G. Enter such other and further relief as may be just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury of all claims so triable.

DATED: August 20, 2021

Respectfully submitted,

HELD & HINES, L.L.P.
Attorneys for Plaintiffs and the Class

/s/ Marc J. Held

2004 Ralph Avenue
Brooklyn, New York 11234
(718) 531-9700
mheld@heldhines.com